

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-288275

(43)Date of publication of application : 10.10.2003

(51)Int.Cl. G06F 12/14
G06F 15/00
G06K 17/00
G06K 19/00

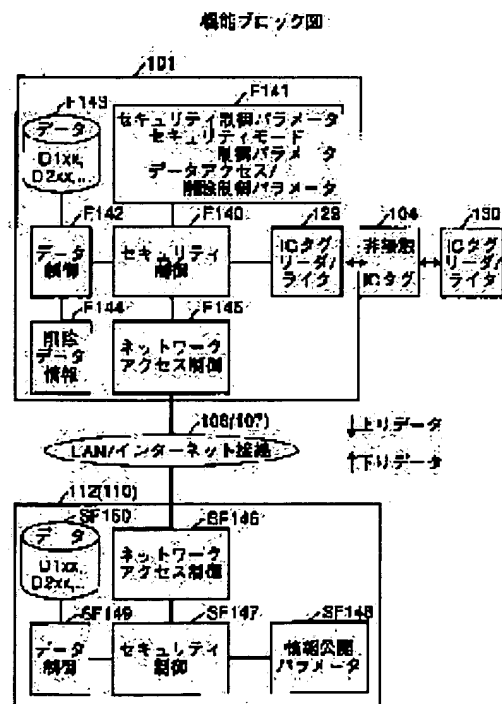
(21)Application number : 2002-093169 (71)Applicant : FUJITSU LTD
(22)Date of filing : 28.03.2002 (72)Inventor : TADANO TORU
NAKAZAWA NOBUHIRO
FURUYAMA MIKIO

(54) INFORMATION SECURITY MANAGEMENT METHOD, PROGRAM FOR EXECUTING IT, AND INFORMATION SECURITY MANAGEMENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To apply information security according to a usage area (location) of a portable computer PC for preventing leakage of information.

SOLUTION: In use of the portable computer PC100 (PC012) transferred between the usage areas S101, S201, and S301, information operation by the computer is restricted in compliance with the usage area of the computer PC100 (PC012). In this case, the information operation is restricted differently in a plurality of divided usage areas S101, S201, and S301. In servers 112 and 110 connected to each other via the computer PC100 (PC012) and networks 106 and 107, information matching the usage areas of the computer is provided, and according, to the usage area of the computer, an offer of information to the computer is restricted.



LEGAL STATUS

[Date of request for examination] 12.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2003-288275

(P2003-288275A)

(43)公開日 平成15年10月10日(2003.10.10)

(51)IntCl. ⁷	識別記号	F I	テマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
15/00	3 3 0	15/00	3 3 0 A 5 B 0 3 5
G 0 6 K 17/00		G 0 6 K 17/00	L 5 B 0 5 8
19/00		19/00	T 5 B 0 8 5

審査請求 未請求 請求項の数5 OL (全11頁)

(21)出願番号 特願2002-93169(P2002-93169)

(22)出願日 平成14年3月28日(2002.3.28)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 只野 徹

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 中澤 信弘

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100089118

弁理士 酒井 宏明

最終頁に続く

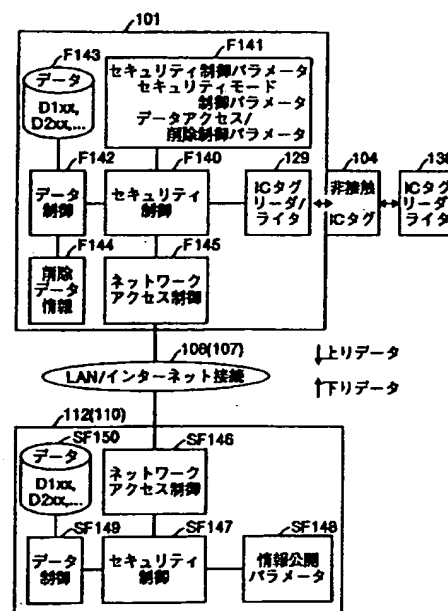
(54)【発明の名称】 情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置

(57)【要約】

【課題】 情報の漏洩を防止するためPCの使用エリア(場所)に応じて情報のセキュリティを施すようにしたこと。

【解決手段】 可搬性あるコンピュータPC100(PC012)を使用エリアをS101、S201、S301という具合に移動して使用するに当たり、コンピュータPC100(PC012)の使用エリアに応じてこのコンピュータによる情報操作に制限を加えるようにした。この場合、複数の区画された使用エリアS101、S201、S301に対してそれぞれ異なる情報操作の制限を行うようにした。また、コンピュータPC100(PC012)とネットワーク106、107を通じて接続されるサーバ112、110上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する。

機能ブロック図



【特許請求の範囲】

【請求項1】 可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加える情報セキュリティ管理方法。

【請求項2】 複数の区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことを特徴とする請求項1に記載の情報セキュリティ管理方法。

【請求項3】 可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する情報セキュリティ管理方法。

【請求項4】 コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加える方法をコンピュータに実行させるプログラム。

【請求項5】 使用エリアに対応してエリア固有信号を出力する発信機を備え、

この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、可搬性あるコンピュータの使用エリアに応じて情報の操作あるいは情報の提供を制限（逆にいえば開放）する情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置に関する。

【0002】

【従来の技術】従来、いわゆるセキュリティシステムは、多くの場所で種々存在し、例えば人の入退室や入退場を制限する人に対するもの、機器の持ち込みや持ち出しを制限する物に対するものが有り、更にはコンピュータやネットワークの分野でのデータやデータ処理に限れば、ID/パスワードやファイルのアクセス制限などコンピュータ単体に関するもの、利用者認証やネットワーク接続経路などサーバデータに関するものが、現実に挙げられる。

【0003】このようなセキュリティシステムにあっては、コンピュータに係るデータ授受及びデータ処理などの情報操作に関するセキュリティは、ID/パスワード等概ね使用者に依存しているのが実状である。従って、使用者の個人認証さえできれば、コンピュータをどこに運んでどこで使用しようがまったく問題はない。殊にネットワークが張り巡らされてどこでもデータの授受やデータの処理が可能となり、一方ノートブック型パーソナルコンピュータ等可搬性あるパーソナルコンピュータ

（以下PCという）が普及する現在、使用者個人のログインさえできればデータの取り出しやデータの処理等PCによる作業はどこにおいても行える。

【0004】

【発明が解決しようとする課題】しかしながら、このような状況においては情報漏洩が問題であり、そしてその最大の原因は、使用者によるものであることを勘案すると、使用者個人の個人認証だけでは情報のセキュリティは不十分である。具体的に例えばPCを外部へ持ち出し、使用者がログインさえできれば情報の取り出し等を容易に行うことができ、PCを故意に持ち出されて悪用されることが十分考えられる。また、例えば可搬性あるPCであって常時ネットワークに接続されたPCにあって、人事異動などによりPCの使用場所が変更された場合には、新たな場所でのセキュリティシステムの変更や指導がネットワーク/サーバ管理者にて行われるが、個人認証だけに依存したのではこの変更や指導までのタイムラグによりセキュリティホールが発生する可能性もある。

【0005】いずれにしても使用者個人による個人認証に依存して、情報のセキュリティを保持することは不十分である。

【0006】この発明は、上述した従来技術による問題点を解消するためになされたものであり、PCの使用エリア（場所）に応じて情報のセキュリティを施すようにした情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1の発明に係る情報セキュリティ管理方法は、ノートブック型あるいはデスクトップ型に係わらず可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作（例えばデータの授受やデータの処理）に制限（セキュリティモードの変更やアクセスの制限あるいはデータの削除）を加えることを特徴とする。

【0008】この請求項1の発明によれば、コンピュータの使用エリアに応じたセキュリティ対策をとることができる。また、リスクの大小によりセキュリティと操作性との関係を適切に融合させることができる。

【0009】また、請求項2の発明に係る情報セキュリティ管理方法は、請求項1の発明において、複数の区画された使用エリアに対してそれぞれ異なる情報操作の制限（セキュリティモードの変更やアクセスの制限あるいはデータの削除）を行うことを特徴とする。

【0010】この請求項2の発明によれば、複数のエリアのリスクの段階に応じたセキュリティ対策をとることができる。

【0011】また、請求項3の発明に係る情報セキュリティ管理方法は、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じて情報公開パラメータを用いてこのコンピュータへの情報の提供を制限することを特徴とする。

【0012】この請求項3の発明によれば、コンピュータの使用エリアに対応するネットワークのサーバ上にある情報の漏洩も防止することができる。

【0013】また、請求項4の発明に係る情報セキュリティ管理方法を実行するプログラムは、コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加えるアプリケーションプログラムとしたことを特徴とする。

【0014】この請求項4の発明によれば、コンピュータ制御プログラムとしてセキュリティ制御プログラムを得ることができる。

【0015】また、請求項5の発明に係る情報セキュリティ管理装置は、使用エリアに対応してエリア固有信号（エリア特定信号を含む）を出力する発信機を備え、この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えたことを特徴とする。

【0016】この請求項5の発明によれば、コンピュータの盗難や持ち出しに対しても有効なセキュリティ対策を講ずることができる。

【0017】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置の好適な実施の形態を詳細に説明する。

【0018】（実施の形態）まず、本実施の形態に係る情報セキュリティ管理方法、この方法を実行するプログラム、及び情報セキュリティ管理装置の前提となるコンピュータシステムについて説明する。図1は、コンピュータシステムの構成図であり、図2はコンピュータシステムのブロック図である。

【0019】同図に示すように、図1に示すコンピュータシステムには、可搬性あるノートブック型PC100の本体部101、本体部101からの指示により表示画面に画像等の情報を表示するディスプレイ102、このコンピュータシステムに種々の情報を入力するためのキーボード103、本体部101の外箱表面に貼付された非接触のICタグ104、ディスプレイ102の表示画面の任意の位置を指定するマウス105、ローカルエリアネットワーク（LAN）106または広域エリアネットワーク（WAN）に接続するLANインターフェース、インターネットなどの公衆回線107に接続するモ

デム108、が備えられている。ここで、LAN106は、ほかのコンピュータシステム111、サーバ112、プリンタ113等とPC100とを接続しており、公衆回線107もサーバ110とモデム108とを接続している。また、図2に示すように、本体部101は、CPU121、RAM122、ROM123、ハードディスクドライブ（HDD）124、CD-ROMドライブ125、FDDドライブ126、I/Oインターフェース127、LANインターフェース128、及びICタグリーダ129を備えている。なお、このICタグリーダは、後述のICタグライタと共用できる同じ製品すなわちICタグリーダ/ライタを用いることができる。

【0020】このコンピュータシステムにおいて使用エリアの情報セキュリティ管理を行おうとする場合、まず、そのエリア（場所）の出入口等に備えられた発信機であるICタグライタ（図1、2では図示省略）によってPC100の本体部101に貼付されたICタグ104にコードが書き込まれる。そして、このコードは、本体部101内に備えられたICタグリーダ129にて読み出される。すなわち、PC100にはそのPC100が存在するエリアのICタグライタ130のコードが読み出されることになる。ICタグリーダ129にて読み出されたコードは、I/Oインターフェース127を介してRAM122に記憶され、CPU121にてエリア（場所）コードに変換されRAM122に記憶される。本体部101ではこのエリアコードに応じて情報セキュリティ制御が行われる。この情報セキュリティ制御は、例えばHDD124にて駆動されるハードディスクに記録されたセキュリティモード制御パラメータあるいはデータアクセス/削除制御パラメータに基づいてセキュリティモードを設定したりデータアクセスを制限したりあるいはデータの削除をするという制御である。また、図1及び図2に示すように本体部101が、LAN106や公衆回線107を通じてサーバ112や110に接続されている場合には、前述の各本体部101に読み込まれたエリアコードに応じた情報セキュリティ制御により、サーバ内の情報公開パラメータに基づきサーバからの情報公開（提供）を制限するという制御も行われる。以上が図1、図2に示すコンピュータシステムを用いた情報セキュリティ管理の概要である。

【0021】次に図3に示す機能ブロックを用いて情報セキュリティ管理装置の詳細を説明する。図3は、図2に示すブロックを情報セキュリティ制御の機能ブロックとして置き換えた図である。図3において、エリア（場所）の出入口等には発信機であるICタグライタ130が備えられる。このICタグライタ130では、書き込み機能にてライタ固有のコードが発信され、換言すればそのICタグライタ130が置かれたエリア固有のコードが発信される。

【0022】他方、PC100の本体部101に貼付さ

れたICタグ104には、ICタグライタ130に近付いたりあるいは通過することによってこのライタ固有コードが書き込まれる。すなわち、PC100を出入口等にて移動させたり通過させることにより非接触のICタグ104に上記固有コードが書き込まれる。

【0023】PC100の本体部101内では、ICタグ104に書き込まれた固有コードを読み出すためのICタグリーダ129が備えられる。セキュリティ制御ブロックF140では、このICタグリーダ129で読み出された固有コードに基づき、セキュリティモードの変更、データアクセス制限の変更、あるいはデータ削除の可否選択からなるセキュリティ制御が行われる。この場合、セキュリティモードの変更、データアクセス制限の変更、あるいはデータ削除の可否選択は、セキュリティ制御パラメータブロックF141によるパラメータに基づく。ここで、セキュリティモードの変更は、具体的にはID、パスワード、あるいはハードディスクパスワード等の選択をいい、データアクセス制限の変更は、例えば秘密の段階に応じたデータへのアクセスの段階的な制限の変更をいい、データの削除の可否選択は、データを削除するかあるいはしないかの選択をいう。

【0024】なお、ICタグライタ130の固有コードのコピーした場合にはこのセキュリティ制御は無効になるので、秘密の段階が高いICタグライタ130には例えば暗号化キーを持たせPC100内にて複合化キーを持たせるようにしても良い。

【0025】また、ICタグライタ130の固有コードを書き込んだICタグ104の固有コードをICタグリーダ129にて読み出した状態では、PC100の使用エリアは特定されないで、エリアを特定するテーブルとかアプリケーションプログラムを備えて複合化キーの照合と共にエリアコードを得るようにしても良い。また更に、ICタグライタ130の固有コード自体をエリア特定コードとすることも可能であり、この場合にはエリア特定のためのテーブルやアプリケーションは不要となる。

【0026】データ制御ブロックF142は、セキュリティ制御ブロックF140の制御情報に応じてデータファイルF143に対するデータ制御を行うもので、ID等が一致してもアクセス制限があれば例えば部分的にしかデータのアクセスができず、更にデータの削除の場合には削除データ情報を記録ブロックF144に記録するというデータ制御を行うものである。なお、削除データ情報記録ブロックF144は、データの削除にてデータを消し去るのではなく、PC100の使用エリアがデータ削除の使用エリアから変化した場合、削除データを復旧させるために備えられたものである。

【0027】また、ネットワークアクセス制御ブロックF145は、セキュリティ制御ブロックF140の制御情報に応じてネットワーク106や107に対するア

セス制御を行うもので、例えばID等が一致しなければネットワークへのアクセスはできない。

【0028】一方、サーバ112や110でも同様に機能ブロックを有し、ネットワークアクセス制御ブロックSF146はネットワーク106や107に対するアクセス制御を行う。セキュリティ制御ブロックSF147では、PC100でのセキュリティ制御ブロックF140でのセキュリティ制御に応じてセキュリティ制御を行うもので、例えばアクセス制限があれば情報公開パラメータブロックSF148のパラメータに基づく部分的なアクセスしかできず、情報の部分的な提供しかできないようになっている。データ制御ブロックSF149は、セキュリティ制御ブロックSF147の制御情報に応じてデータファイルSF150に対するデータ制御を行うものである。なお、図3においては、PC100のネットワーク106や107への接続を前提として説明したが、PC100を単独で使用する場合にはサーバ112や110への情報公開パラメータのアクセス制限は存在しない。

【0029】図4は、PC100の使用エリアとして一つの部屋S501を想定し、この部屋S501にPC100を持ち込んだり持ち出したりするケースを示している。すなわち、通常PC100を使用する部屋S501では、使用者の個人認証のみにて何らアクセスの制限なく使用できる場合でも、このPC100を出入口を通過して持ち出そうとした場合には出入口付近に設置されたICタグライタ130i及び130eから送信される固有コードによりPC100内のセキュリティ制御が実行され、例えばPC100内のデータファイルF143のデータを削除データとして、部屋S501外のPC100ではデータの取り出しや処理を不可能にすることができる。また逆に、部屋S501内のPC100を一旦部屋S501外に出したが再度部屋S501内に運び込む場合には、ICタグライタ130i及び130eから送信される固有コードにより削除データとするセキュリティ制御が外れ元のまま使用者の個人認証のみにて何らアクセスの制限なく使用できるようにもできる。また、外部から別の場所のPC100が持ち込まれた場合には、新品のPCを除いて、LANに接続した場合、サーバ112からのデータを削除データとするセキュリティ制御をしても良い。このように同じPC100の同じエリアへの持ち出しや持ち込みを繰り返す場合には、固有コードの履歴を見ることによって、セキュリティ制御を実行したり外すことでエリアのセキュリティの保持と復旧が可能になる。

【0030】ここで、セキュリティ制御の実行時期は、PC100の移動後PC100の起動時であったり、あるいはPC100の起動中定期的に行うことができる。

【0031】また、部屋S501の出入口付近に備えたICタグライタ130i、130eは出入口の内と外と

に備えたが、これはPC100の出入口の通過の確認と移動の方向の確認のためのものであり、PC100のICタグ104にICタグライタ130iと130eとの内外双方のコードが記録されれば通過となり、この場合130iの固有コードが先に記録され130eの固有コードが後の場合は持ち出し、逆の場合は持ち込みとなる。また、片方のICタグライタ130iあるいは130eのみの固有コードの記録の場合はそのICタグライタ側のエリアにICタグすなわちPC100が存在することになる。この出入口内外のICタグライタ130iと130e双方の配置は、近づくことによってICタグ104にコードが記録される種類のICタグにとって、通過と移動方向の両者を記録するには有効である。もっとも、一つのICタグライタ130でもPC100の通過と移動方向が記録でき伴別できるICタグ104の場合には、すなわち通過することによってのみ移動方向が記録されるICタグ104の場合には、ICタグライタを二つ備える必要はない。このようにICタグライタは固有コードを発信し、その固有コードをICタグは記録するものであるが、要はICタグ引いてはPC100の存在位置がICタグライタの固有コードによって特定できれば良い。

【0032】図5は、PC100の使用エリアとして三つの部屋S101(関係者外秘エリア)、S201(社内事務エリア:顧客立入り不可エリア)、S301(社内オープンエリア:顧客立入り可エリア)と外部エリアS202(外部事務所の事務エリア)を想定し、この部屋S101からPC100を持ち出すケースを示している。なお、この図5に示す例でも図4の説明が基礎となっている。すなわち、PC100の持ち出しのみならず持ち込みもあること、持ち出しと持ち込みの繰り返しもあること、セキュリティ制御の実行時期は起動時も起動中の定期的な時でもよいこと、ICタグライタ130とICタグ104との方式は近づくことで記録したり通過することで記録する方式があること、については、図5の例でも準じて適用される。

【0033】この図5の例では、主にセキュリティ制御の詳細について述べる。この例では、図4の例と同じようにICタグライタは部屋S101、S201、S301の出入口の内外両側に設けられる例を示している。今、PC100が、部屋S101から部屋S201を経て部屋S301に至る場合を述べる。この図5では、便宜上PC100をそのコードPC012で表し、ICタグ104をそのコードIC123にて表し、ICタグライタ130i及び130eをそのコードG1i、G1e、G2i、G2e、G3i、G3e、G4i、G4eにて表す。

【0034】図5において、部屋S101に存在するPC012は部屋S101の出入口の通過にて固有コードG1i、G1eがIC123のタグに記憶され、ついで

次の出入口の通過にて固有コードG2i、G2eがIC123のタグに記憶される。この状態では、PC012は部屋S301に存在する。この経過を図6に示すデータ構造図上、(A)ICタグに関する履歴ではタグIC123にてコードG1i、G1eが記録されてPC012内では部屋S101からS201への移動が確認され、更にコードG2i、G2eが記録されてPC012内では部屋S201からS301への移動が確認される。従って、PC012のセキュリティ制御ブロックF140ではエリアコードS201そしてS301(便宜上部屋の符号とエリアコードを同じ表示とする)が入力される。

【0035】PC012がこのような経過を辿る移動をすることによって、セキュリティモードを変更する場合、図6のデータ構造図上、(B)セキュリティモード変更パラメータでは、エリアコードS101にてモードM1の特定個人の「ID」入力要、エリアコードS201ではモードM2の「無し」である認証不要、エリアコードS301ではモードM3の「ID/パスワード」入力要、というようなモード変更が行われる。なお、このセキュリティモード変更パラメータでは、エリアコードS401ではモードM4の「ID/パスワード/ハードディスクパスワード」入力要、エリアコード不明(ICタグが剥がれる等)では起動不可というモード変更となっている。

【0036】また、PC012がこのような移動をすることによって、データアクセス制限やデータの削除をする場合、図6のデータ構造図上、(C)データアクセス/削除制御パラメータでは、エリアコードによってアクセスが可能あるいは不可能なデータコード、並びに削除が要あるいは不要なデータコードが選択される。また、図6(D)に基づけばデータコードD1では顧客信用調査情報等の関係者外秘情報、データコードD2では顧客取引情報等の社外秘情報、データコードD3では顧客担当者情報等の社外持ち出し禁止情報、データコードD4では顧客公開情報等の公開情報が対応する。従って、図6(C)によれば、データコードD1、D2、D3、D4について、エリアコードS101は全データコードD1、D2、D3、D4にアクセス可能で削除は要しないエリアであり、エリアコードS201はデータコードD1につきアクセス不可能あるいは削除を要しかつデータコードD2、D3、D4につきアクセス可能あるいは削除は要しないエリアであり、エリアコードS301はデータコードD1、D2につきアクセス不可能あるいは削除を要しかつデータコードD3、D4につきアクセス可能あるいは削除は要しないエリアである。更に、エリアコードS401はデータコードD1、D2、D3につきアクセス不可能あるいは削除を要しかつデータコードD4につきアクセス可能あるいは削除は要しないエリアであり、エリアコード不明では全データコードD1、D

2、D3、D4につきアクセス不可能あるいは削除を要する非常事態となっている。こうして、PC012が社外に至るに従い、アクセスが不可能な情報が増え、削除を要する情報が増大する。

【0037】ここで、一般に秘密の要求が高い情報は操作性が煩雑で管理も厳重となり、逆に公開性の高い情報は操作しやすく管理も容易となるのであるが、これまで一般に行われてきたセキュリティ対策は、秘密の要求が高い情報に対して必要以上に操作性を悪くしたり管理負荷が過度であったり、反面に秘密の要求が高い情報であっても、操作性を優先するあまり脆弱となっているという状況が見受けられる。本実施の形態では、図5での部屋の構成に基づいて図6(B)(C)の制御パラメータを設定しており、これらの説明から判明するように例えば情報漏洩のリスクが大きければセキュリティを優先し、このリスクが少なければ操作性を優先するというセキュリティと操作性とのトレードオフの関係を適切に融合させている。

【0038】図7(A)は、PC012が使用エリアを移動することによって削除すべきデータ情報の履歴を示したもので、エリアコードに対応してデータコードが削除される。すなわち、エリアコードS201が得られる場合つまり部屋S201にPC012が移動した時データコードD1の情報が削除される。更に、部屋S301にPC012が移動してエリアコードS301となった時はデータコードD2の情報が削除される。この図7の削除データの履歴は、図6(c)に示す削除制御パラメータのデータ構造とも一致している。

【0039】図7(B)はPC012が移動した後ネットワークに接続した場合、サーバ側での情報公開パラメータを示しており、PC012の移動により得られたエリアコードに対応して図7(C)に示すデータコードを選択して公開可能あるいは不可能としたり、削除した場合には復元可能あるいは不可能とするものである。この場合、削除データを復元可能とすることは、エリアデータの変更にて削除されていたデータをPC012からの復元要求にてアクセス可能とし復元データを公開(提供)することである。この図7(B)の情報公開パラメータ及び図7(C)のデータコードの内容は、図6(C)(D)と同じであり説明は省略する。

【0040】図8(A)は、セキュリティ制御での制御処理を示したフローチャートである。図8(A)において、まずICタグに書き込まれた固有コードからエリアコードを求め(ステップST1)、次いで電源起動時のセキュリティ制御の場合には、セキュリティコードに対応するセキュリティモードを起動する(ステップST2)。ステップST3にてデータ制御がない場合は、フローの終了となるが、データ制御を行う場合には、ステップST4にてデータの削除があるかどうかの判断をする。データの削除がない場合には、アクセス制御である

ので、エリアコードに対応するアクセス不可データのアクセスを禁止する(ステップST5)。一方データの削除がある場合には、エリアコードに対応する削除データを削除し削除データ情報に書き込む(ステップST6)。なおこのフローチャートで電源起動時のセキュリティ制御をしないで、定期的なセキュリティ制御にチェックを行う場合には、ステップST2は不要となる。

【0041】図8(B)はICタグからのコード書き込みフローチャートを示し、まずICタグライタからICタグにゲート情報である固有コードが書き込まれる(ステップST10)。次いで、本体内にて固有コードから対応するエリアコードに変換する(ステップST11)。その後セキュリティ制御が実行される(ステップST12)。

【0042】上述してきたように、本実施の形態1では、ICタグライタ130、ICタグ104、ICタグリーダ129によって固有コードを得てセキュリティ制御を行うものであったが、GPSの衛星からの送信信号を受信する受信機をPCに搭載すれば、この位置情報もしくは、位置情報と時刻との組合せを利用して、PCの使用エリアを特定することによってセキュリティ制御を行うことができる。この場合、位置情報に正確を期すためにディファレンシャルGPSを適用することも可能である。

【0043】なおここでは、PC012の使用エリアを検出し、その使用エリアに応じてこのPC012による情報操作に制限を加える方法を実行させるプログラム、つまり図3の機能を前提として図6、図7に基づき図8のフローチャートをコンピュータに実行させるプログラムを得ることができる。

【0044】本実施の形態によれば、PC012の使用エリア(場所)に応じて情報操作に制限を加えるようにできたので、PC012の使用エリアとセキュリティの段階に応じた情報のセキュリティ制御を行うことができた。

【0045】(付記1)可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加えることを特徴とする情報セキュリティ管理方法。

【0046】(付記2)複数の区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことを特徴とする付記1に記載の情報セキュリティ管理方法。

【0047】(付記3)コンピュータによる情報操作の制限はセキュリティモードを変更して行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0048】(付記4)コンピュータによる情報操作の制限はデータアクセスを制限して行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0049】(付記5) コンピュータによる情報操作の制限はデータを削除して行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0050】(付記6) 削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする付記5に記載の情報セキュリティ管理方法。

【0051】(付記7) コンピュータの使用エリアの特定は、使用エリアに対応して発信機から出力されるエリア特定信号であることを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0052】(付記8) コンピュータの使用エリアの特定は、GPSの衛星から送られた受信信号に基づいて行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0053】(付記9) コンピュータの使用エリアの特定は、コンピュータ起動時に行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0054】(付記10) コンピュータの使用エリアの特定は、コンピュータ起動中周期的に行うことを特徴とする付記1または2に記載の情報セキュリティ管理方法。

【0055】(付記11) 可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限する情報セキュリティ管理方法。

【0056】(付記12) コンピュータへの情報の提供の制限は、セキュリティモードに応じて行うことを特徴とする付記11に記載の情報セキュリティ管理方法。

【0057】(付記13) コンピュータへの情報の提供の制限は、データアクセスを制限して行うことを特徴とする付記11に記載の情報セキュリティ管理方法。

【0058】(付記14) コンピュータへの情報の提供の制限は、データを削除して行うことを特徴とする付記11に記載の情報セキュリティ管理方法。

【0059】(付記15) 削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする付記14に記載の情報セキュリティ管理方法。

【0060】(付記16) コンピュータへの情報の提供の制限は、使用エリアに対応して発信機から出力されるコンピュータからのエリア特定信号に基づいて行うことを特徴とする付記11に記載の情報セキュリティ管理方法。

【0061】(付記17) コンピュータへの情報の提供の制限は、コンピュータから送られるGPSからの受信信号に基づいて行うことを特徴とする付記11に記載の情報セキュリティ管理方法。

【0062】(付記18) コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによ

る情報操作に制限を加える情報セキュリティ管理方法をコンピュータに実行させるプログラム。

【0063】(付記19) コンピュータによる情報操作の制限はセキュリティモードを変更して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0064】(付記20) コンピュータによる情報操作の制限はデータアクセスを制限して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0065】(付記21) コンピュータによる情報操作の制限はデータを削除して行うことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0066】(付記22) 削除したデータは、コンピュータの使用エリアに応じて復旧可能としたことを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記21に記載のプログラム。

【0067】(付記23) コンピュータの使用エリアは、使用エリアに対応して発信機から出力されるエリア特定信号を検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0068】(付記24) コンピュータの使用エリアは、GPSの衛星から送られた受信信号に基づいて検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0069】(付記25) コンピュータの使用エリアは、コンピュータの起動時に検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0070】(付記26) コンピュータの使用エリアは、コンピュータの起動中周期的に検出することを特徴とする情報セキュリティ管理方法をコンピュータに実行させる付記18に記載のプログラム。

【0071】(付記27) 使用エリアに対応してエリア特定信号を出力する発信機を備え、この発信機からのエリア特定信号を受信する受信機を有しかつこの受信機により受信したエリア特定信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【0072】(付記28) 発信機はICタグリーダライタであり、受信機は非接触ICタグである付記27に記載の情報セキュリティ管理装置。

【0073】(付記29) GPSの衛星からの送信信号を受信する受信機を有し、この受信機によりコンピュータの使用エリアを特定しかつこの使用エリアに応じて情報操作の制限を行う制御回路を有するコンピュータを備えた情報セキュリティ管理装置。

【0074】(付記30) 受信機はディファレンシャル

GPSに基づいて構成される付記29に記載の情報セキュリティ管理装置。

【0075】

【発明の効果】以上説明したように、請求項1の発明によれば、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、コンピュータの使用エリアに応じてこのコンピュータによる情報操作に制限を加えることにより、コンピュータの使用エリアに応じたセキュリティ対策をとることができ、リスクの大小によりセキュリティと操作性との関係を適切に融合させることができるという効果を奏する。

【0076】また、請求項2の発明によれば、複数の区画された使用エリアに対してそれぞれ異なる情報操作の制限を行うことにより、複数のエリアの段階に応じたセキュリティ対策をとることができるという効果を奏する。

【0077】また、請求項3の発明によれば、可搬性あるコンピュータを使用エリアを移動して使用するに当たり、このコンピュータとネットワークを通じて接続されるサーバ上にコンピュータの使用エリアに対応する情報を有し、コンピュータの使用エリアに応じてこのコンピュータへの情報の提供を制限することにより、コンピュータの使用エリアに対応するネットワークのサーバ上にある情報の漏洩も防止することができるという効果を奏する。

【0078】また、請求項4の発明によれば、コンピュータの使用エリアを検出し、その使用エリアに応じてこのコンピュータによる情報操作に制限を加えるプログラムであることにより、コンピュータ制御プログラムとしてセキュリティ制御プログラムを得ることができるという効果を奏する。

【0079】また、請求項5の発明によれば、使用エリアに対応してエリア固有信号を出力する発信機を備え、この発信機からのエリア固有信号を受信する受信機を有しかつこの受信機により受信したエリア固有信号に応じて情報操作の制限を行う制御回路を有するコンピュータを備えたことにより、コンピュータの盗難や持ち出しに対しても有効なセキュリティ対策を講ずることができるという効果を奏する。

【図面の簡単な説明】

【図1】本実施の形態に係るコンピュータシステムの概略を示す構成図である。

【図2】本実施の形態に係る図1のコンピュータシステムのブロック図である。

【図3】本実施の形態に係る機能ブロック図である。

【図4】コンピュータの単一使用エリアを示す構成図である。

【図5】コンピュータの複数使用エリアを示す構成図である。

【図6】データ構造図である。

【図7】データ構造図である。

【図8】セキュリティ機能のフローチャートである。

【符号の説明】

100、PC100、PC012 コンピュータ

101 本体部

104 ICタグ

106 ネットワーク

107 公衆回線

110、112 サーバ

20 129 ICタグリーダー

130、130i、130e、G1i、G1e、G2

i、G2e、G3i、G3e、G4i、G4e ICタグライタ

F140、SF147 セキュリティ制御ブロック

F141 セキュリティ制御パラメータブロック

F142、SF149 データ制御ブロック

F143、SF150 データファイル

F144 削除データ情報ブロック

SF148 情報公開パラメータブロック

30 S101、S201、S301、S202、S501 部屋

IC123、PC012、S101、S201、S30

1、S202、G1i、G1e、G2i、G2e、G3

i、G3e、G4i、G4e、M1、M2、M3、M

4、D1、D2、D3、D4 コード（なお、説明の便

宜上

PC012、S101、S201、S301、S20

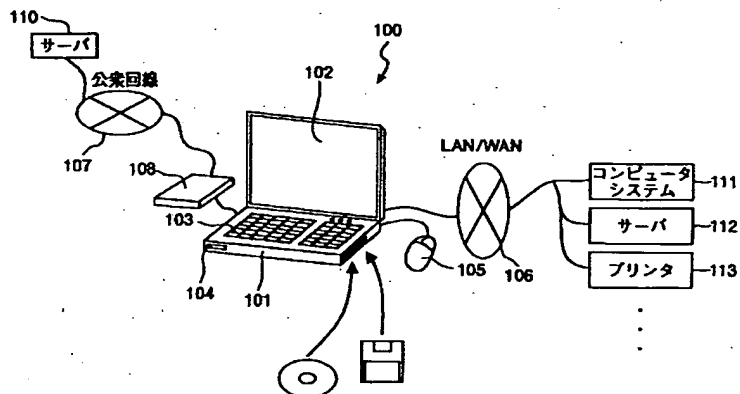
2、G1i、G1e、G2i、G2e、G3i、G3

e、G4i、G4e、はコードと装置（ここではPC、

40 部屋、ICタグライタ）の表示を兼用する。）

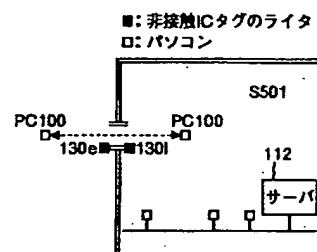
【図1】

コンピュータシステムの概略構成図



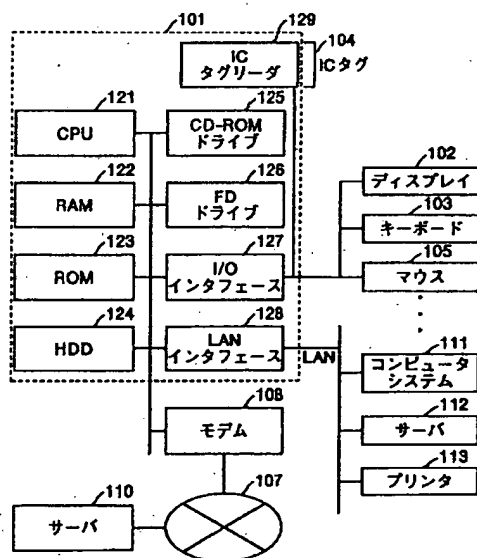
【図4】

単一使用エリアの構成図



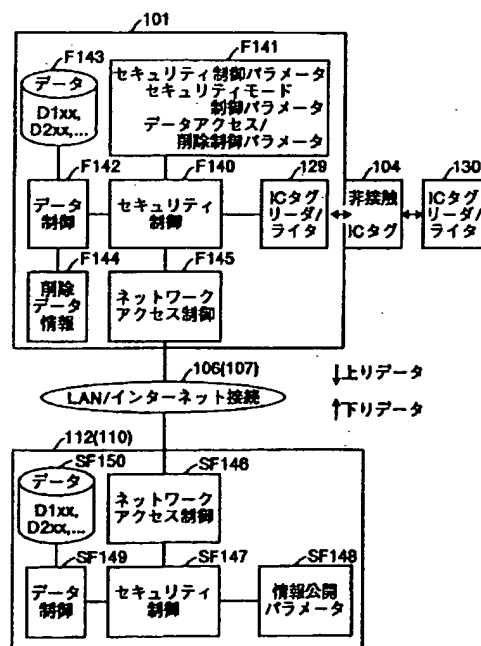
【図2】

コンピュータシステムのブロック図



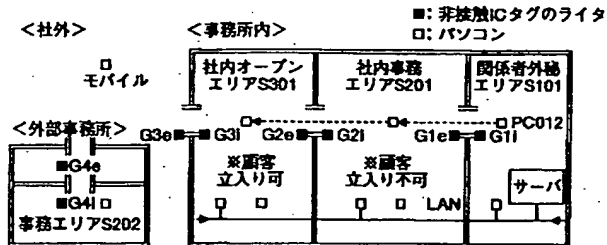
【図3】

機能ブロック図



【図5】

複数使用エリアの構成図



【図6】

データ構造図

(A) 非接触ICタグに関する履歴

IC コード	PC コード	エリア履歴		ゲート情報	
		コード	名称	コード	年月日時分秒
IC123	PC012	S301	社内 オープンエリア	G2e, G3i	020204103145
...	...	S201	社内事務 エリア	G1e, G1i	020204090255
...

(B) セキュリティモード制御パラメータ

エリア		セキュリティモード	
コード	名称	コード	セキュリティ機能の例
S1xx	関係者外秘エリア	M1	ID入力
S2xx	社内事務エリア	M2	無し
S3xx	社内 オープンエリア	M3	ID/パスワード入力
S4xx	社外エリア	M4	ID/パスワード、 ハードディスクパスワード入力
不明	非常事態	XX	起動不可

(C) データアクセス/削除制御パラメータ

エリア		データコード			
エリア	名称	D1	D2	D3	D4
S1xx	関係者外秘 エリア	○	○	○	○
S2xx	社内事務エリア	×	○	○	○
S3xx	社内 オープンエリア	×	×	○	○
S4xx	社外エリア	×	×	×	○
不明	非常事態	×	×	×	×

○: アクセス可、又は削除不要
×: アクセス不可、又は削除要

(D) データコードの例

コード	セキュリティレベル	情報の例
D1xx	関係者外秘	顧客信用調査情報
D2xx	社外秘	顧客取引情報
D3xx	社外持ち出し禁止	顧客担当者情報
D4xx	公開情報	顧客公開情報

【図7】

データ構造図

(A) 削除データ情報

IC コード	PC コード	削除情報		
		エリア	ファイル名	年月日時分秒
IC123	PC012	S301	顧客取引情報	D2xx 020204104545
...
...	...	S201	顧客信用調査情報	D1xx 020204091530
...

(B) 情報公開パラメータ

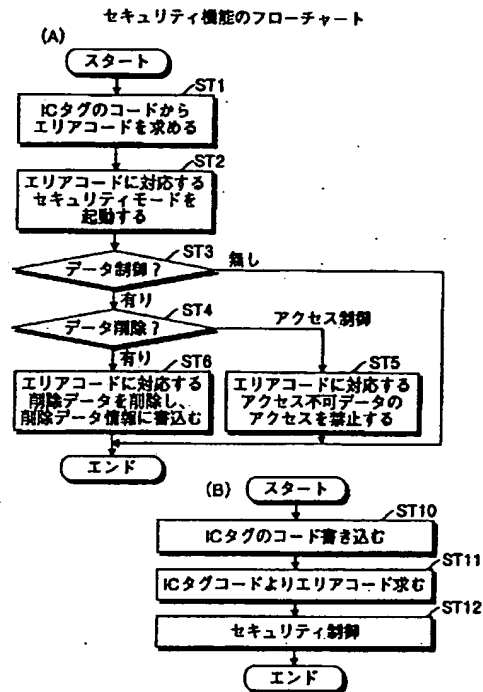
エリア		データコード			
コード	名称	D1	D2	D3	D4
S1xx	関係者外秘エリア	○	○	○	○
S2xx	社内事務エリア	×	○	○	○
S3xx	社内オープンエリア	×	×	○	○
S4xx	社外エリア	×	×	×	○
不明	非常事態	×	×	×	×

○: 公開可、又は復元可
×: 公開不可、又は復元不可

(C) データコードの例

コード	セキュリティレベル	情報の例
D1xx	関係者外秘	顧客信用調査情報
D2xx	社外秘	顧客取引情報
D3xx	社外持ち出し禁止	顧客担当者情報
D4xx	公開情報	顧客公開情報

【図8】



フロントページの続き

(72)発明者 古山 幹雄
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA06 BB09 BB10
5B035 BB09 BC00 CA23
5B058 CA15 KA02 KA04 YA20
5B085 AE00 AE06 AE11

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☒ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.